An Incentive-Compatible Routing Protocol for Two-Hop Delay-Tolerant Networks

Ying Cai, *Member, IEEE*, Yanfang Fan, and Ding Wen

***Abstract*—Delay-tolerant networks (DTNs) rely on the mobility of nodes and their contacts to make up with the lack of continuous connectivity and, thus, enable message delivery from source to destination in a "store–carry–forward" fashion. Since message delivery consumes resource such as storage and power, some nodes may choose not to forward or carry others' messages while relying on others to deliver their locally generated messages. These kinds of selfish behaviors may hinder effective communications over DTNs. In this paper, we present an efficient incentive-compatible (IC) routing protocol (ICRP) with multiple copies for two-hop DTNs based on the algorithmic game theory. It takes both the encounter probability and transmission cost into consideration to deal with the misbehaviors of selfish nodes. Moreover, we employ the optimal sequential stopping rule and Vickrey–Clarke–Groves (VCG) auction as a strategy to select optimal relay nodes to ensure that nodes that honestly report their encounter probability and transmission cost can maximize their rewards. We attempt to find the optimal stopping time threshold adaptively based on realistic probability model and propose an algorithm to calculate the threshold. Based on this threshold, we propose a new method to select relay nodes for multicopy transmissions. To ensure that the selected relay nodes can receive their rewards securely, we develop a signature scheme based on a bilinear map to prevent the malicious nodes from tampering. Through simulations, we demonstrate that ICRP can effectively stimulate nodes to forward/carry messages and achieve higher packet delivery ratio with lower transmission cost.**

***Index Terms*—Delay-tolerant networks (DTNs), incentive compatibility, optimal sequential stopping rule, routing protocol.**

I. Introduction

DUE to the tremendous popularity of smartphones and their diverse uses in various applications, mobile data traffic has been exponentially increasing, resulting in serious congestion in wireless networks, particularly in cellular systems. Traditional network resource and end-to-end data delivery mechanisms are no longer effective in handling steadily increasing traffic. Considering the steadily increasing data traffic over cellular networks, the only possible way to address traffic congestion without adding network resource is to transport delay-tolerant data traffic via opportunistic strategy to off-load traffic at a less-congested area. However, some relays do not forward the message for other nodes since message delivery consumes resource such as storage and power. Therefore, we need an incentive mechanism to stimulate the node to forward the message to deal with the misbehavior of selfish nodes. A delay-tolerant network (DTN) is a mobile wireless ad hoc network, where end-to-end path does not exist at any given moment or is hard to maintain [1]–[3]. Message delivery relies on opportunistic encounters of mobile nodes and is accomplished in the "store–carry–forward" fashion. For example, the in-transit message, called bundles, as shown in Fig. 1, could be forwarded when two nodes move within each other's transmission range in DTNs. If no other node is within the transmission range of node A, node A will buffer the current bundles and carry them until other node appears within its transmission range. Therefore, the "store–carry–forward" routing, which depends on the mobility of nodes and their encounters, makes up with the lack of continuous connectivity and thus enables message delivery from source to destination by intermittent connections [4]–[7]. Obviously, DTNs can be used to reduce the traffic load on the traditional infrastructure networks. In the field of file sharing and bulk data transmissions [8]–[10], successful practical applications of DTNs have been deployed.

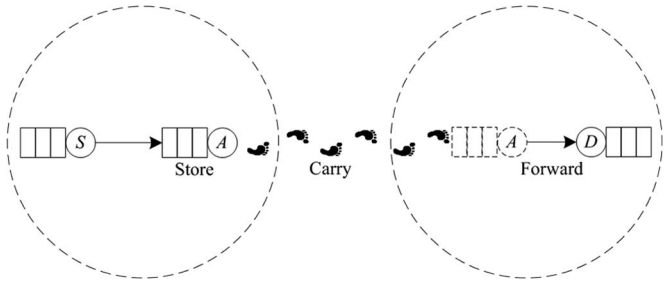

Fig. 1. Store–carry–forward in DTNs.

As aforementioned, nodes deliver messages in the "store–carry–forward" fashion in DTNs. The two-hop relaying algorithms and their variants [3], [11] have led to a set of elegant routing protocols with high efficiency and simplicity. In a two-hop relay routing algorithm, a message travels from source S at most two hops to arrive at its destination D either from the source S directly or from one of the other distinct relays. The relay node will forward the packet when the destination D is in the transmission range; otherwise, the relay node will drop the packet since only source S can decide packet relaying.

Manuscript received December 27, 2014; revised April 6, 2015; accepted June 11, 2015. Date of publication July 8, 2015; date of current version January 13, 2016. This work was supported in part by the Open Project of the State Key Laboratory of Information Security under Grant 2014-16, by Beijing Key Laboratory of Internet Culture and Digital Dissemination Research under Grant ICDD201408, by Beijing Higher Education Young Elite Teacher Project under Grant YETP1499, and by the National Natural Science Foundation of China under Grant 61373038. The review of this paper was coordinated by Prof. J. Sun.

Y. Cai is with the Beijing Key Laboratory of Internet Culture and Digital Dissemination Research, Beijing Information Science and Technology University, Beijing 100101, China, and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: ycai@bistu.edu.cn).

Y. Fan and D. Wen are with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: fyfhappy@bistu.edu.cn; wendinglong@sina.com).

Digital Object Identifier 10.1109/TVT.2015.2454291

Since all nodes in a two-hop relaying algorithm are required to forward messages for each other in a cooperative and altruistic way, a critical issue in this kind of cooperation is how to deal with energy consumption and storage at each node. An intuitive idea to reduce energy consumption and storage cost is to enable all nodes to cooperate with each other willingly [9], [10], [12] when they have opportunities to deliver messages. Unfortunately, in practice, nodes may act selfishly, particularly when their energy and storage resource are limited. In a data relay process, a selfish node may report false encounter probability to others to avoid being selected as a relay node. This kind of selfish misbehavior can deteriorate the network performance and even crumble normal network operations. Therefore, we investigate how to deal with such selfish behaviors for two-hop DTNs.

In this paper, we focus on a two-hop relaying routing problem, which delivers any packet at most two hops to arrive at the destination in DTNs in which nodes may be selfish. Incentive mechanisms typically have been designed to stimulate cooperation and fight against selfish behaviors. Here, we intend to use incentive as well to deal with our problem. We propose an efficient incentive-compatible (IC) routing protocol (ICRP) with multiple copies for two-hop DTNs by using optimal sequential stopping rule [13] and algorithmic game theory [14]. A source node chooses a relay node with the maximum reward according to the optimal sequential stopping rule and determines the reward value by algorithmic game theory. We show that relaying nodes can receive the maximum reward only when they honestly report the true encounter probability and routing metrics, which will stimulate nodes to participate in the relay node selection process. To guarantee true reporting, we employ the Vickrey–Clarke–Groves (VCG) auction (second-price sealed-bid) [15]–[17] as a strategy to refine the relay node selection process, in which the bidder with the highest price will win but only the second highest price is rewarded. When a node refuses to forward messages for others, it will not receive reward, which means that it may not get relaying services from others in the future. This way, selfish behaviors (e.g., discarding or refusing to forward messages) can be mitigated.

Our main contributions can be summarized as follows.

1) We investigate relay-based routing protocols in two-hop DTNs with the existence of selfish nodes. We propose an IC protocol, where relaying nodes are chosen based on the optimal sequential stopping rule.
2) We find the optimal stopping time threshold adaptively based on a realistic probability model and propose an algorithm to calculate the threshold. Based on this threshold, we propose a new method to select relay nodes for multicopy transmissions.
3) To defend against forgery attacks in DTNs, we propose a new payment method by the use of virtual currency and bilinear pairing in our ICRP.
4) We evaluate our protocol through experiments and show that our ICRP can effectively handle the selfish behaviors in DTNs while achieving higher message delivery ratio with lower cost.

The remainder of this paper is organized as follows. Section II reviews works related to incentive schemes and optimal stopping problem in DTNs. Section III presents the system model and design objectives. We elaborate the proposed protocol in Section IV. Evaluation and performance analysis are carried out in Section V. Finally, Section VI concludes this paper.

II. Related Works

The initial research in DTNs focuses on how to design efficient message delivery schemes based on opportunistic transmissions. Most papers assume that there are no selfish nodes in the sense that each node forwards messages for others [3], [18]. There are indeed some works addressing node selfishness issues [19], [20]. A promising approach to deal with node selfishness issue and stimulate node cooperation among nodes is to use the incentive scheme. All research works along this line can be roughly divided into two categories, i.e., the reputation-based schemes and credit-based schemes.

In the first category, reputation-based schemes rely on individual nodes to monitor neighboring nodes' traffic and keep track of the reputation of each other so that uncooperative nodes can be eventually detected and excluded from networks [12]. These techniques have been used to improve the performance of DTNs because honest nodes can be chosen to carry and forward packets in the reputation-based schemes.

In the second category, credit-based schemes can be characterized in two different ways: online and offline. Online credit-based schemes mainly use some form of virtual currency to reward and punish nodes to stimulate cooperation among nodes. Some schemes do require nodes to pay fee (virtual currency) to receive messages and charge more for more relays, but they do need an online credit authority to deal with payment management [21]. On the other hand, offline credit-based schemes mainly introduce layered coins issued by offline credit authority [20], [22], [23].

There are many reputation-based and credit-based incentive protocols for wireless ad hoc networks proposed in the current literature [24]–[28]. Due to precious transmission opportunities, it should transfer data as far as possible whenever transmission opportunity presents. Unfortunately, because of the unique feature of DTNs, it is hard to detect selfish behaviors of nodes in DTNs, which makes the existing incentive protocols for wireless ad hoc networks difficult to use in DTNs directly. Because of the mobility of nodes in DTNs, we observe that the selection process of relay nodes is similar to the classical secretary problem in optimal sequential stopping rule [13]. When encountering a node, a source node must determine whether to choose it as a relay node, and once determining it is not suitable, the node will no longer participate in this transmission opportunity. There are two ways to solving the secretary problem. The first way is to choose the candidate that ranks the first according to a certain optimality criterion [29]. The second way is to choose the first node whose decision parameter is greater than a threshold as the relay node. The threshold value is determined by observing and calculating certain candidates' performance metric. We use the latter method to choose the

relay node by taking both the encounter probability and the transmission cost into consideration in this paper.

Khosravi [30] considered the case of packet transmissions with single copy for relay node selection under a threshold (observed before), which is determined by the encounter probability, but the author only takes the probability into consideration while neglecting the transmission cost, leading to selfish behaviors. Tsuruike *et al.* [29] proposed choosing a mobile relay node with higher delivery probability by applying the solution to the secretary problem, an optimal sequential stopping rule without recall, which minimizes the expected rank of the selected observation. Different from previous studies, Wen *et al.* [31] designed an incentive protocol by jointly considering the transmission cost and encounter probability to defend against selfish behaviors. In our preliminary work [32], we assumed that the optimal stopping time threshold is constant and runs the algorithm with the same stopping time threshold during the whole routing process for a message. Unfortunately, in practice, it is expected that the threshold will not be constant and will depend on the network dynamic. Thus, in this paper, we attempt finding the optimal stopping time threshold adaptively based on a realistic probability model and propose an algorithm to calculate the threshold. Based on this threshold, we propose a new method to select relay nodes for multicopy transmissions. Moreover, we carry out extensive numerical studies based on Opportunistic Network Environment (ONE) [33]. Finally, to defend against malicious attacks, we also design a security mechanism based on bilinear pairing.

III. System Model and Design Objectives

Assume that the system operates in discrete time with time period matching the timescale of traffic distribution. We now describe the models we use in this paper to defend against selfish behaviors and stimulate cooperation among nodes. We will discuss the network model, node model, mobility model, and attack model in the next few sections. The notations used in this paper are listed in Table I as follows.

TABLE I
Notations

Notation	Description
p_{ij}	Encounter probability between node i and j
c_{ij}	Packet transmission cost between node i and j
θ_i	Parameter information of node i
$\hat{\theta}_i$	Parameter information of node i report
u_i	Expected payment after node i reports θ_i
$\hat{u}_i$	Expected payment after node i reports $\hat{\theta}_i$
S	Source node
D	Destination node
N_i	Relay node
$r_i(\hat{\theta},\mu)$	Reward for node i as the relay node
μ	Actual completion status
Sig_S	Signature of node S
$Cert_S$	Certificate of S generated by OSM
V^*	Comparison value of the expected payment

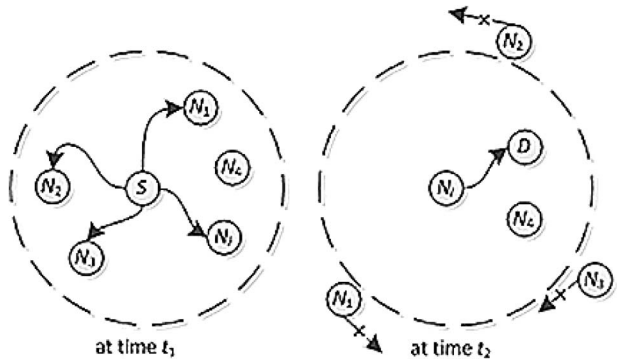

Fig. 2. Two-hop transmissions in DTNs, where an arrow represents an opportunistic link, a cross represents packet dropping, and a dashed circle represents a transmission range.

A. DTN Model

We characterize a DTN model by a directed graph $G = (V, E)$, where V is the set of nodes and E is the set of edges that connect nodes with probability. As shown in Fig. 2, packets are transferred in a two-hop fashion, where a source node S delivers packets to a destination node D via one relay node. Nodes (such as smartphones) can communicate over infrastructured networks (e.g., Third-Generation (3G) networks) or point-to-point wireless access networks (e.g., Bluetooth and Wi-Fi). To reduce the load on the backbone network, nodes can only access to infrastructured networks when transferring control messages (e.g., registration and payment). Other messages are delivered through point-to-point wireless access networks. We assume that there exists an offline security manager (OSM) and a virtual bank (VB). The OSM is responsible for key management. Every node must register with the OSM and get a public key certificate before joining the DTN. The VB is responsible for virtual currency management, storing the payment from source nodes, and paying relay nodes. We assume that every node in the DTN can have access to the VB through the infrastructured network and get the payments after receiving the ACK messages from the destination nodes for a successful data delivery. Virtual currency can be rewarded for packet forwarding service. If a node does not participate in packet delivery, it will not get any virtual currency, which means that it may not receive services from other nodes.

B. Node Model

In a DTN, for each node i, let p_{ij} denote the encounter probability between node i and node j, and let c_{ij} denote the nonnegative transmission cost for a packet to be delivered from node i to node j. Define the parameter vector $\theta_i = (p_i, c_i)$, where $p_i = (p_{i1}, p_{i2}, p_{i3}, \ldots)$ and $c_i = (c_{i1}, c_{i2}, c_{i3}, \ldots)$. The parameter vector can be regarded as the private information for each node. When a source node wants to send a packet, the node willing to forward will report its parameter and compete for the transmission opportunity. Since nodes rely on virtual currency to gain network services (forwarding help from other

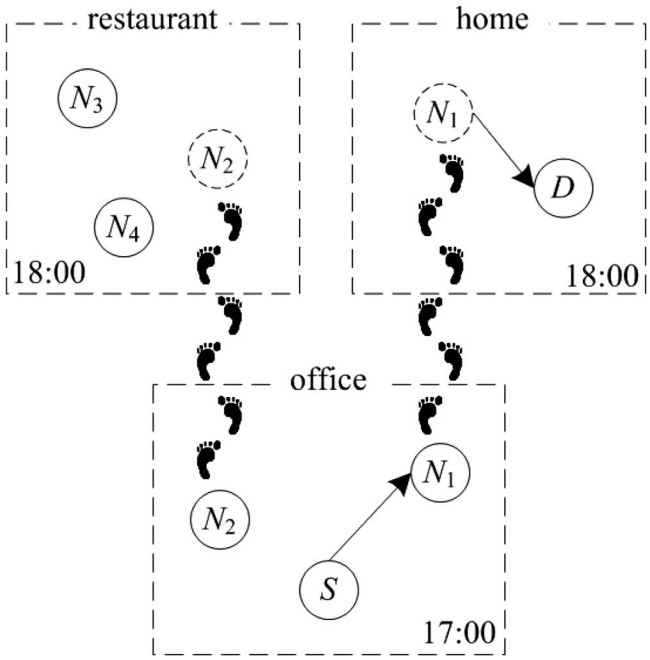

Fig. 3. Example of a movement model.

nodes), malicious nodes may report false parameters to win the competition. To defend against this, we design an incentive scheme to encourage nodes to report true parameters and prove that this is the best choice for each node to win the opportunity in Section IV.

C. Mobility Model

User mobility is determined by human behaviors since nodes in DTNs are made up of mobile devices carried by humans. The moving behavior of humans in the social environment has certain regularity. For example, students often appear in the dormitory, classrooms, and dining rooms. Workers often go back and forth between their homes and offices. Therefore, it is reasonable to model node mobility as the user movement. Because data transmission delay is significantly shorter when compared with that of the inter-contact time between nodes, we can neglect such a transmission delay when characterizing mobility. Thus, we assume that nodes exchange data directly when they are in the same building, whereas they cannot do so when in different buildings. Taking the movement of students, for example (as shown in Fig. 3), node S in the dormitory wants to send packets to node D in the dining room. It can choose one of other nodes in the dormitory as a relay and carry and forward the packets to D when it arrives at the dining room.

D. Attack Model

There are two typical types of uncooperative nodes, namely, selfish nodes and malicious nodes in DTNs. Selfish nodes are reluctant to forward packets destined for other nodes when not compensated or seek to economically maximize their own benefits. Malicious nodes attempt to attack the system by interrupting the normal network operations and/or attempt to obtain more virtual currency without actually forwarding packets. Consequently, there are two kinds of potential threats with which we have to deal.

1) Does Not Forward: A node does not participate in forwarding or reports false parameters to win forwarding opportunity but does not forward data intentionally.

2) Forgery Attack: A node may forge a fake ACK to get reward from the VB, although it does not help in successful transmission.

E. Design Objectives

As previously discussed, our design objectives must meet the following requirements.

1) IC: If node i has parameter θ_i with the expected payment u_i, when it reports parameter $\hat{\theta}_i$ with the expected payment $\hat{u}_i$, $u_i \geq \hat{u}_i$ always holds according to the dominant strategy for each node to report the true parameter.

2) Individual Rational: Each node always has a nonnegative expected payment, i.e., $u_i \geq 0$.

3) Security: The protocol should be able to defend against the forgery attack.

F. Attack Model

To address security issue, we need some cryptographic technique such as bilinear pairing [34]. Denote an additive cyclic group by G_1, a multiplicative cyclic group of the same prime order q by G_2, and a generator of G_1 by P. A bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear map that satisfies the following conditions.

1) Bilinear: $e(aP, bP) = e(P, P)^{ab}$ for all $a, b \in Z_q^*$.

2) Nondegenerate: $e(P, P) \neq 1$ for all $p \in G_1$.

3) Computable: Map $e(P, Q)$ is efficiency computable for any $P, Q \in G_1$.

IV. Proposed Protocol

Here, we first give the overview of our proposed protocol, followed by a detailed description. We first provide the optimal cutoff threshold algorithm, which is the algorithmic foundation of relay node selection. Then, we introduce the relay node selection algorithm and the protocol analysis.

A. Overview of ICRP

In this paper, we limit the two-hop relay from a source to its destination, i.e., a source only uses one relay node to its destination. When source node S wants to send a packet to destination node D, nodes near S that would like to be the relay node will report their own parameters θ_i to S. S selects a relay node based on the algorithm of choosing an intermediate node. A packet is transferred in the form of bundle [22]. As shown in Fig. 4, after S sends a packet to the relay node, S sends the virtual currency and relay node's identity information to VB. Destination node D sends an ACK when successfully receiving the packet from the relay node. The relay node gets the payment after VB verifies the ACK and the id information

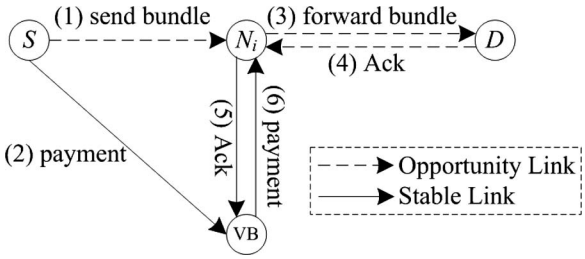

Fig. 4. Process of ICRP.

of the relay node. In addition, if the relay node does not forward successfully within the specified time, VB will return the virtual currency to node S.

B. Detail of Our Proposed Protocol (ICRP)

From the design objectives and overview, we describe the proposed protocol in detail. Here, we present our routing protocol in the following steps: system initialization, bundle generation, relay node selection, bundle forwarding, and bundle verification.

1) System Initialization: The system parameters (q, G_1, G_2, e, P, H) of the OSM include the bilinear pairing system parameters (q, G_1, G_2, e, P) and a hash function, which is defined as follows: H: $\{0,1\}^* \rightarrow G$. The system parameters will be preloaded in every DTN node. For any node to join the DTNs, it randomly chooses $SK_N \in Z_q^*$ as its private key corresponding to public key expressed as $PK_N = SK_N P$ and the OSM issues its corresponding public key certificate. All these should be done during the initial interaction between the node and the OSM.

2) Relay Node Selection: The source has to choose an appropriate relay node from potential candidates. Due to its importance and complexity, we will postpone the selection algorithm later, which is in fact one of the major contributions of this paper.

3) Bundle Generation: A packet is transferred in the form of bundle. When source node S sends bundle B to destination node D, after determining the relay node N_i, S signs on the bundle with its private keys SK_S by computing $Sig_S = SK_S H(B_k||S||D||TS||TTL||N_i)$, where TS and TTL refer to the bundle creation timestamp and time-to-live information, respectively, and B_k is the bundle containing the kth duplicate of a packet. Then, S sends the parameters $B_k, S, D, TS, TTL, Sig_S, Cert_S$ to relay node N_i.

4) Bundle Forwarding: When the relay node receives the bundle B, it first checks whether the bundle is within its lifetime. If so, it adds certificate $Cert_{N_i}$ into the bundle; otherwise, it discards the bundle. The relay node N_i will forward the bundle B to destination D when it meets D.

5) Bundle Verification: When destination D receives the bundle, it also first checks whether the bundle is within its lifetime. If the bundle does not expire, D verifies the validity of $Cert_S$ and $Cert_{N_i}$. After this, it verifies if $e(P, Sig_S) = e(PK_S, H(B_k||S||D||TS||TTL||N_i))$ holds. This equation does not hold if one of these parameters $B_k, S, D, TS, TTL, Sig_S, Cert_S$ is modified. The destination node D discards the bundle if this verification fails. After all the verifications pass, D sends back the ACK packet containing ID of the duplicate bundle and the relay node identity to relay node N_i that can prove this relay node forwards the bundle for S successfully. At the same time, the VB can get the ACK packet from the destination D. Then, N_i gets the payment from the VB.

C. Optimal Threshold Selection Algorithm

The challenge in designing our protocol is to guarantee the incentive compatibility and individual rationality for multiple duplicate transmissions. Moreover, we observe that the selection of the relay node is similar to the classical secretary problem of optimal stopping theory [13]. Optimal stopping time threshold r is a very important parameter for the classical secretary problem. To find the optimal threshold, we first study some basic probabilities of interest.

1) Optimal Cutoff Threshold for Relay Selection: Single-Copy Case: Our problems involve time t and node x that capture the "state of affairs." We deal only with the case in which node x moves while there are a total of m_i nodes in the set S_i around the transmission range at the time $t_i (i = 1, \ldots, m)$. Assume that source x meets a total of n nodes in which x moves within the period of time t, and then, n is equal to the cardinal number of the sets $S_1 \cup S_2 \cup \cdots \cup S_m$, $t = t_1 + t_2 + \cdots + t_m$. We call these n nodes as candidates in the DTNs in which the source could use them to carry and forward messages. The problem to be discussed in this paper is to allow the source node more than one choice to select the best candidate as the relay node. We will derive the optimal cutoff threshold r^*, which maximizes the probability of finding the best relay node.

Definition 1: Assume that source node S meets a total of n candidates in the network in the time of interest, a cutoff threshold r is referring to the value that objects are compared for optimality until r objects are reached, and then the first encountered object right after the rth object with a better value than the optimal value among the first r objects will be chosen as the final choice.

Remark 1: The optimality here is based on a certain metric. For the relay problem, which will be elaborated later, the metric is the reported parameter for forwarding capability. Moreover, the definition of cutoff threshold r means that, given r, find the optimal choice among the r objects, and then the final choice will be the first encountered object afterward. For the relay selection scenario, we first find the best relay node among the r relay candidates, then we search for the next relay node, which is better than this optimal node, and then, we stop the search. This is the optimal stopping rule, which we formally formulate as follows.

Strategy 1: For a given cutoff threshold r, we first find the optimal relay node among the r relay candidates. Starting from the $(r+1)$th relay node, if we first find any relay node better than the aforementioned discovered optimal node, then we use this newly discovered relay node as the final choice and stop the selection process.

先从r个candidate里找到最优node, 再从r+1开始, 找到一个node比刚刚最优的那个relay还好，就把这个新发现的作为final choice

This strategy has the following property.

Lemma 1: For given n candidate nodes in the DTNs and a given cutoff threshold r in Strategy 1, A_j denotes the event that the jth node is the final choice in Strategy 1 and p_r denotes the probability that the final choice in Strategy 1 is the optimal relay node among the n candidate nodes. Then, $p_r = (r/n)\sum_{j=r+1}^{n}(1/j-1)$.

Proof: Since $\{A_j\}_{r+1\le j\le n}$ are obviously pairwise disjoint, $p_r = \sum_{j=r+1}^{n} P(A_j)$

$$P(A_j) = \begin{cases} \frac{1}{n}, & j = r+1 \\ \frac{r}{j-1}\cdot\frac{1}{n}, & j > r+1 \end{cases} = \frac{r}{j-1}\cdot\frac{1}{n}$$

$$p_r = \frac{r}{n}\sum_{j=r+1}^{n}\frac{1}{j-1}.$$

Obviously, the choice of the cutoff threshold r plays an important role. When $r = 0$, the final choice can be any relay node, hardly an optimal node. When $r = n$, we examine all candidate nodes, and the final choice is for sure the optimal node, but computation may be high. In our prior research [31], we used experiments to determine appropriate value r. Here, we will find the optimal cutoff threshold r^*. ■

Lemma 2: For given n candidate nodes in the DTNs, there exists an r^*, which maximizes p_r, and it is given by $r^* = \max\{r : \sum_{j=r+1}^{n}(1/j-1) > 1\}$.

Proof: It is easy to derive that

$$p_r - p_{r-1} = \frac{1}{n}\left(\sum_{j=r+1}^{n}\frac{1}{j-1} - 1\right).$$

Thus, $p_r > p_{r-1}$ iff $\sum_{j=r+1}^{n}(1/(j-1)) - 1 > 1$, and hence, $r^* = \max\{r : \sum_{j=r+1}^{n}(1/(j-1)) > 1\}$ maximizes p_r. ■

Remark 2: r^* is dependent on n. When n is large, r/n denoted by x, then we can approximate p_r as $p_r = x\int_x^1(1/t)dt = -x\cdot\ln x$, from which we can obtain the optimal value of x as $x = (1/e)$. Therefore, $r^* = (n/e)$, and $p_{r^*} = (1/e)$.

Remark 3: Here, we assume that n candidates are known. However, we may not be able to predict how many nodes one encounters beforehand in the DTNs. Many times, we may have to use estimation to roughly estimate the number of relay nodes. In [31], we have selected a constant r and make some comparisons for different r. Next, we present our approach to evaluating the optimal cutoff threshold r^* for multicopy message delivery.

2) Optimal Cutoff Threshold for Relay Selection—Multicopy Case: The previous section deals with only a single-copy message delivery system in which a single relay node is needed. To increase the message delivery efficiency, it has been proposed to use a multicopy message delivery mechanism in the sense that a message is sent to multiple relay nodes. Here, we generalize the previous technique to multicopy scenario, and the idea is to find the optimal cutoff threshold for finding multiple, e.g., k, relay nodes. Similar to our previous argument on secretary problem, we need to find the probability that k better selections after comparing r candidate nodes are top-k optimal among n candidate nodes. It turns out that this problem is the extreme value problem of a single variable when n and k are known.

Strategy 2: As in Strategy 1, we first compare first r nodes and find the optimal value. Afterward, find the next k better candidate nodes (which have better bidding than this optimal value), and then stop the search and choose these k nodes as the relay nodes.

Lemma 3: Assume that there are n candidates in the DTNs, uniformly distributed, and source node S intends to send k copies for delivery. Then, the probability that the discovered k candidates are the top-k optimal candidates is given by $P_r = k\times\sum_{i=r+k}^{i=n}((1/n)\times(C_{i-r-1}^{k-1}/C_{n-1}^{k-1})\times(r/(i-k)))$.

Proof: Assume that variable i represents the last relay selection. Then, according to node distribution assumption, it is one of the top-k nodes with probability $(1/n)$. The other $k-1$ nodes are between r and $i-1$. Then, there are $C_{i-r-1}^{k-1}\times A_{k-1}^{k-1} = C_{i-r-1}^{k-1}\times(k-1)!$ permutations and combinations for these $(k-1)$ nodes among the nodes between $(r+1)$ and $(i-1)$. Observe that the total number of these $(k-1)$ nodes among $(n-1)$ nodes is given by $C_{n-1}^{k-1}\times A_{k-1}^{k-1} = C_{n-1}^{k-1}\times(k-1)!$. Thus, the probability of finding the discovered $(k-1)$ nodes is $(C_{i-r-1}^{k-1}/C_{n-1}^{k-1})$. Moreover, the probability that a node selected is under 1 and r is $(r/(i-k))$. Furthermore, we notice that variable i is an integer from $r+k$ to n. Applying the theorem of total probability, we obtain the probability that the k selected nodes from Strategy 2 are the top-k optimal candidates given by $P_r = k\times\sum_{i=r+k}^{i-n}((1/n)\times(C_{i-r-1}^{k-1}/C_{n-1}^{k-1})\times(r/(i-k)))$, where $n > r+k$.

This completes the proof. ■

The optimal probability can be calculated using the iterative algorithm given subsequently to obtain the optimal cutoff threshold r^*.

Algorithm 1 Calculation of the Optimal Cutoff Threshold r

Input:
the number of candidates: n and the number of copies: k
Output:
the optimal cutoff threshold r^*
1: Let optimal probability variable $OV = 0$
2: **for** $r = 1$ to $i = n-k$ **do**
3: $P_r = k\times\sum_{i=r+k}^{i=n}((1/n)\times(C_{i-r-1}^{k-1}/C_{n-1}^{k-1})\times(r/(i-k)))$
4: **if** $P_r > OV$
5: $OV \leftarrow P_r$
6: **else**
7: Output r
8: **end if**
9: **end for**

D. Relay Node Selection

One challenge in choosing the relay nodes above is how to design the competition schema to select the best relay forwarding messages when a payment-based incentive mechanism is used to stimulate node participation in DTNs. Moreover, when

nodes have to collect enough credits or virtual currency to gain services from DTNs, relay nodes may report overrated parameters such as higher encounter probability and/or lower transmission cost to win the competition for credits. In the previous section, we assume that all relay nodes report their honest parameters based on which the best relay nodes can be selected. To overcome false reporting, we employ the VCG auction [15]–[17] as a strategy to refine the relay node selection process, in which the bidder with the highest price will win but only the second highest price is rewarded. In this sense, we choose the relay node with the highest expected payment but pay the second highest price. Thus, we can prevent the node report from overrated forwarding capability reporting.

Source node S can give payment when its message is delivered to the destination node successfully. Assume that V represents a source's current amount of virtual currency, which will be used to reward those relaying nodes that help the source to forward its message successfully. When it needs to send a message, it estimates the expected virtual currency by $p_i \cdot V - c_i$ for node i when S receives parameters (p_i, c_i) from neighbor i. It then chooses relay candidate nodes using the following algorithm.

Algorithm 2 Relay Nodes Selection

Input:
(n, k) represent the numbers of nodes and copies, respectively
Output:
relay nodes and expected payments
for $f = 1$ to $f = k$ **do**
  Execute Algorithm 1
  Execute Procedure 1 //the node with the maximum virtual currency among r nodes
  Let $V^* \leftarrow \arg\max_r(\hat{p}_r, V_f - \hat{c}_r)$
  Execute Procedure 2 // searching for the relay node which is the first better node after r nodes inspection
  Let $i \leftarrow (\hat{p}_i \cdot V - c_i \geq V^*)$
  $P = k \times \sum_{i=r+k}^{i-n}((1/n) \times (C_{i-r-1}^{k-1}/C_{n-1}^{k-1}) \times (r/(i-k)))$
  $r_i(\hat{\theta}_i, \mu) = V_k \cdot \mu - V^*$
  for all $j \neq i$ **do**
    $f(\hat{\theta}_j) = 0$
    $r_j(\hat{\theta}_j, \mu) = 0$
  end for
end for

Procedure 1 Calculate the Maximum Virtual Currency

for $i = 1$ to $i = r^*$ **do**
  // r^* represents the optimal cutoff threshold
  if$(\hat{p}_i \cdot V - c_i \geq V^*)$ **then**
    $V^* = \hat{p}_i \cdot V - c_i$
  end if
  $f(\hat{\theta}_i) = 0$
  $r_i(\hat{\theta}_i, \mu) = 0$
end for

Procedure 2 Search for the Relay Node

for $i = r + 1$ to $i = n$ **do**
  // n represents the numbers of total nodes
  if $(\hat{p}_i \cdot V_i - c_i \geq V^*)$ **then**
    Count $++$;
    //the numbers of relay nodes to be selected
    $f(\hat{\theta}_i) = 1$
    $r_i(\hat{\theta}_i, \mu) = V_i \cdot \mu - V^*$
    count $\geq k$ **then**
      //k represents total numbers of message copies
      Break;
    end if
  else
    $f(\hat{\theta}_i) = 0$
    $r_i(\hat{\theta}_i, \mu) = 0$
  end if
end for

V_k refers to the source node's virtual currency after the destination node receives bundle B_k successfully, and function $f(\hat{\theta}_i)$ is a Boolean variable that records the set of bundles to node i when it reports $\hat{\theta}_i$ and whether it wins the competition. Let $r_i(\hat{\theta}_i, \mu)$ denote the reward that node i can get, and let μ denote the actual completion status, which is independent of $\hat{\theta}_i$. Let $\mu = 1$ if node i forwards bundles B_k successfully, and $\mu = 0$ if node i fails to complete the transmission successfully.

To justify our approach, we need to find the optimal cutoff threshold r^* and compare with what we discover from our approach. We select a constant r and find V^* from a number of r nodes, which is equal to $\max_r(\hat{p}_r \cdot V_k - \hat{c}_r)$. After this, we select the first node whose calculated value is greater than V^* from the $(r+1)$th node. In the previous section, we have shown that the probability that the discovered relay node from Strategy 1 is also the optimal relay node is $p_r = (r/n)\sum_{j=r+1}^{n}(1/(j-1))$, and the maximum probability is $p_r = (1/e)$ when $r = (n/e)$ when n is sufficiently large.

After the first copy is sent, the source node S sends the second copy when the transmission opportunity comes, and S stops sending the packet when the destination node receives one copy successfully.

As a final node, in our relay node selection process, we assume that the source knows the number of nodes it encounters. Unfortunately, when choosing relay nodes, the source may not know exactly how many nodes they can encounter at the time of selection. However, various kinds of prediction algorithms can be designed based on the historical contact information on different pairs of nodes. In the simulation study, we examine different values of r and find that there is a range in which the performance can be optimized.

E. Protocol Analysis

As stated previously ICRP stimulates bundle forwarding by rewarding each relay node with the virtual currency for the service they provide while charging the source for the service they receive. It is the unique way that the node with virtual currency

is forwarding messages for other nodes. There is no service provided for a selfish node without virtual currency. Here, we show that our ICRP meets the design objectives successfully, and Algorithm 2 meets the first two design objectives.

Theorem 1: Our protocol ICRP and Algorithm 2 meet *individual rational (IR)* requirement.

Proof: Let the true parameter and the reported parameter of node i be denoted by $\theta_i = (p_i, c_i)$ and $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$, respectively. Let the expected rewards of node i be denoted by u_i and $\hat{u}_i$, respectively, with these parameters.

1) If node i wins the competition for relying based on the true parameter, then $p_i V_k - c_i \geq V^*$. If node i successfully delivers the message, its reward is $V_k - V^*$, whereas if it fails, its payment is $-V^*$, i.e., V^* is lost. The expected payment (we will use the payment and the reward interchangeably) can be calculated as follows:

$$\begin{aligned} u_i &= p_i(V_k - V^*) - (1 - p_i)V^* - c_i \\ &= p_i \cdot V_k - c_i - V^* \geq 0. \end{aligned} \tag{1}$$

   If node i fails in the competition, then $u_i = 0$.

   Therefore, $u_i \geq 0$ when node i reports the true parameter.

2) Assume now that node i reports the true parameter $\theta_i = (p_i, c_i)$, but it fails in the competition, whereas it wins the competition when reporting $\hat{\theta}_i = (\hat{p}_i, \hat{c}_i)$ instead, which means that $p_i \cdot V_k - c_i < V^*$, $\hat{p}_i \cdot V_k - \hat{c}_i \geq V^*$.

   Although it wins the competition based on $\hat{\theta}_i$, its actual reward is calculated according to θ_i. Thus

$$\begin{aligned} \hat{u}_i &= p_i(V_k - V^*) - (1 - p_i)V^* - c_i \\ &= p_i \cdot V_k - c_i - V^* < 0. \end{aligned} \tag{2}$$

   If node i reports $\hat{\theta}_i$ and fails in the competition, the expected reward is $\hat{u}_i = 0$. Therefore, the expected payment $\hat{u}_i \leq 0$ when node i reports false parameter.

   In conclusion, we show that a relay node can ensure a nonnegative expected reward only when reporting the true parameter. Hence, our proposed protocol is *IR* compatible and so is algorithm 2, the foundation of our protocol. ■

Theorem 2: Our protocol ICRP and Algorithm 2 are *IC*.

Proof:

1) If both θ_i and $\hat{\theta}_i$ win the competition for relaying, then $u_i = \hat{u}_i$ because the expected payment is calculated according to the true parameter in this situation.
2) If θ_i wins the competition while $\hat{\theta}_i$ fails, then $u_i > 0$, $\hat{u}_i = 0$, i.e., $u_i > \hat{u}_i$.
3) If θ_i fails and $\hat{\theta}_i$ wins, then $u_i = 0$, $\hat{u}_i$ is calculated according to the true parameter as follows:

$$\begin{aligned} \hat{u}_i &= p_i(V_k - V^*) - (1 - p_i)V^* - c_i \\ &= p_i \cdot V_k - c_i - V^* < 0. \end{aligned} \tag{3}$$

   Thus, $u_i > \hat{u}_i$.
4) If neither θ_i nor $\hat{\theta}_i$ wins, then $u_i = \hat{u}_i = 0$.

TABLE II
SIMULATION SCENARIO SETTINGS

Category	Parameters	Value
Scenario features	Simulation time/h	12
	Simulation area/m	4500×3400
	Background city	Helsinki
Node features	Total number of nodes	126
	Movement speed$\left(m \cdot s^{-1}\right)$	0.5 1.5
	Packet lifetime(h)	5
	Transmission radius(m)	10
	Buffer size(MB)	5

In conclusion, for all nodes, reporting the true parameter is always the best strategy. ■

Theorem 3: ICRP can defend against forgery attack.

Proof: The destination D can use SK_S to verify whether a received bundle has been tampered

$$\begin{aligned} e(P, Sig_S) &= e\left(P, SK_S H\left(B_k \| S \| D \| TS \| TTL \| N_i\right)\right) \\ &= e\left(P, H\left(B_k \| S \| D \| TS \| TTL \| N_i\right)\right)^{SK_S} \\ &= e\left(SK_S P, H\left(B_k \| S \| D \| TS \| TTL \| N_i\right)\right) \\ &= e\left(PK_S, H\left(B_k \| S \| D \| TS \| TTL \| N_i\right)\right). \end{aligned} \tag{4}$$

If any element of the bundle has been tampered, then (4) does not hold. The destination node D will send ACK to relay node only when (4) holds. Moreover, the VB will decrypt the received ACK to ensure the integrity of the payment information in the bundle. ■

V. PERFORMANCE EVALUATION

Here, we evaluate the performance of our proposed protocol ICRP through simulations. We first describe the simulator and system parameters used in this paper. Then, we show the optimal cutoff threshold algorithm related to the numbers of copies and candidates in the DTNs. We use the delivery ratio, the average delay, and the overhead ratio as the performance metrics in our simulation study. These performance metrics vary with respect to different selfishness ratios and the number of copies.

A. Experimental Setup

For the purpose of illustration, we implemented the ICRP in ONE [33], which is a Java-based developmental environment for DTNs and is object oriented and discrete event driven, a popular simulator for DTNs. It can simulate the real network environment well. The system parameter settings, including features of scenarios and nodes, are summarized in Table II. We denote the network delivery ratio, the network average delay, and the overhead ratio by delivery_prob, delay_average, and overhead_ratio, respectively. For each case, we run the simulation ten times to obtain the average delivery_prob, delay_average, and overhead_ratio.

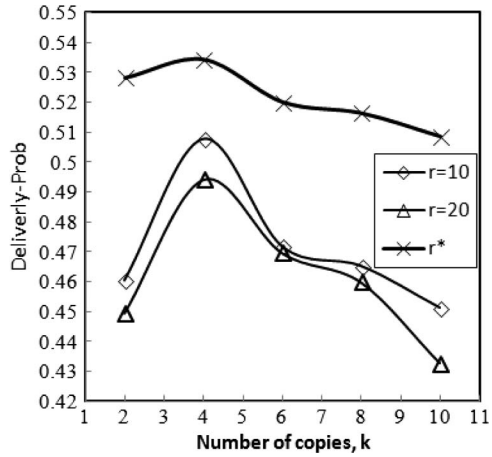

Fig. 5. Comparison between the use of fixed r and the use of the optimal r^* for the delivery ratio with respect to the number of copies.

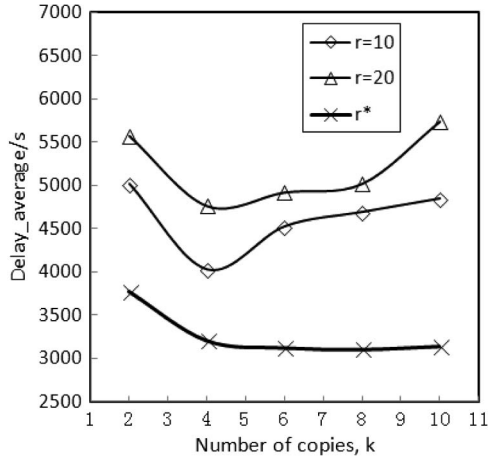

Fig. 6. Comparison between the use of fixed r and the use of the optimal r^* for the delay results with respect to the number of copies.

B. Performance Evaluation

The three performance metrics $delivery\_prob$, $delay\_average$, and $overhead\_ratio$ are rigorously defined as follows. The $delivery\_prob$ is defined as

$$delivery\_prob = \frac{delivered}{created}. \tag{5}$$

Here, we denote the total number of generated packets by *created* and the number of packets successfully delivered to the destination by *delivered*.

The *delay_average* is defined as the average latency of packets that are successfully delivered to the destination. The *overhead_ratio* is defined as

$$overhead\_ratio = \frac{relayed - delivered}{delivered}. \tag{6}$$

Here, *created and delivered* are the same as above. We denote the actual total forwarding times by *relayed*.

To capture the selfishness issue, we define the selfishness ratio by $\alpha = ((the\ number\ of\ selfish\ nodes)/(the\ total\ number\ of\ nodes))$ among these DTN nodes, which is a variable in terms of population of selfish nodes in the network.

1) Limited Number of Message Copies and the Range of r: The node's buffer size is limited; hence, the number of copies could not be increase uncontrollably. We need to limit the number of copies to achieve better performance. In addition, the value of r must be properly selected. It is hard to choose the optimal node if the value of r is too small. On the other hand, if r is too large, the computation for V^* may take too long to find a node whose value is greater than V^*. In this case, it is possible that no node meets the condition, and the packets are transmitted only when the source node encounters the destination node. Therefore, we first analyze the optimal cutoff threshold r^* and fixed r and compare the effect on the number of copies for the delivery ratio and the average delay by using the stimulation study. Then, we fix the number of the copies to analyze the impact on the outcome by varying r. Thus, we can determine a reasonable number of copies and the range of r.

In Figs. 5 and 6, it is observed that, when we fix the value of r, the number of copies around 4 can give higher

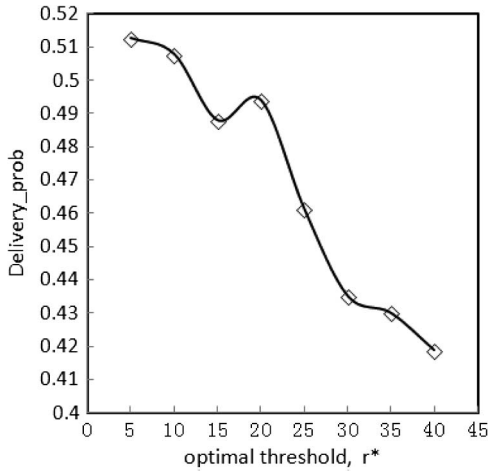

Fig. 7. Relationship between $delivery_{prob}$ and r^*.

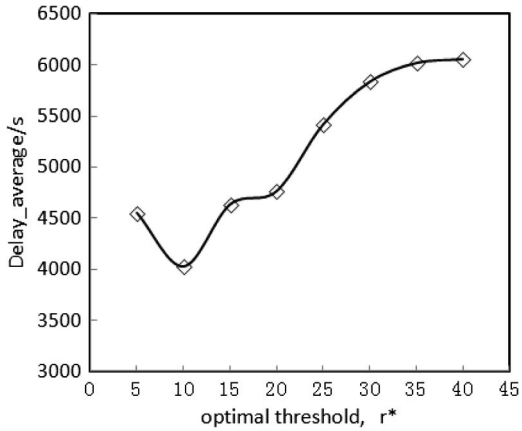

Fig. 8. Relationship between $delay_{average}$ and r^*.

delivery_probability, whereas the *delay_average* is relatively low. For the optimal threshold r^*, similar results can be observed. With the increase in the number of copies, the node's buffer size is limited. More copies will cause network congestion and degrade the network performance.

In Figs. 7 and 8, we can see that, with a fixed number of copies at 4, when r varies from 5 to 40, higher success ratios

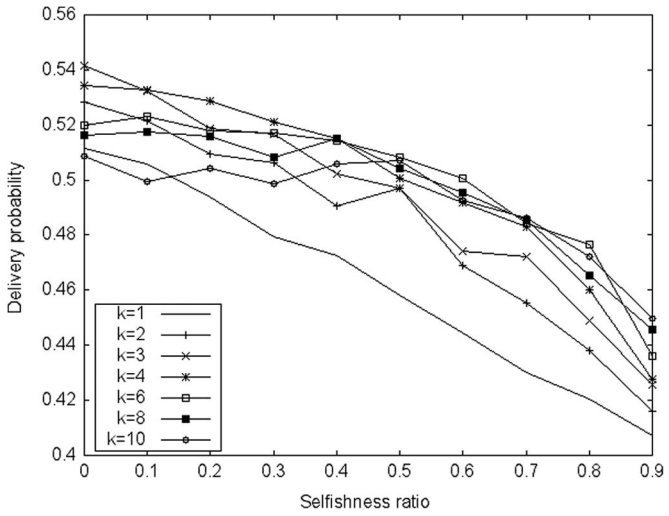

Fig. 9. Comparison of $delivery_{prob}$.

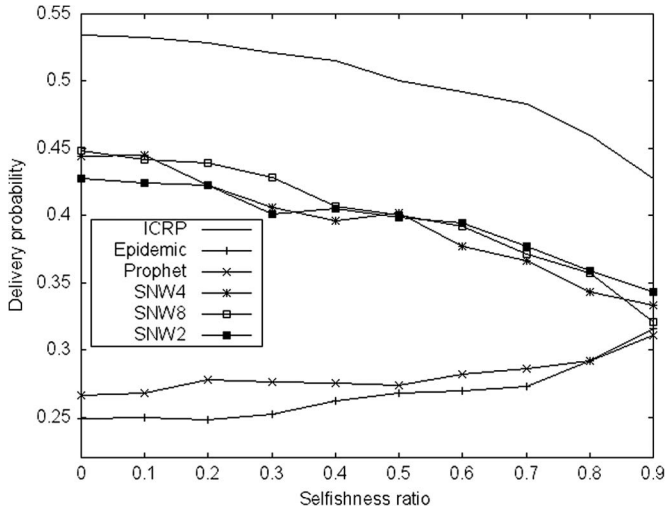

Fig. 10. Comparison of $delivery_{prob}$ among ICRP, Spray and Wait, Epidemic, and PROPHET protocols.

and lower path delivery delay can be achieved. Because, in the simulation environment, it is unknown how many nodes each node will encounter, we can hardly determine an exact value of r through theoretical derivation. Through the experiment results, we can determine an optimal value range.

2) Defending Against Selfish Behavior: We introduce the selfishness ratio into the simulation study and analyze the results of transmission cost under different numbers of copies. Moreover, we compare the performance of ICRP with three well-known existing protocols, Spray and Wait [35], Epidemic [36], and PROPHET [37]. As we previously defined, selfishness ratio α is a variable, and in our simulation, we first generate a random number N_r for a node; if $N_r < \alpha$, then the node is selfish and it may refuse to forward packets for others. When $N_r \geq \alpha$, the node will faithfully forward packets if it has a chance and participates in the competition for relaying to meet the destination node within transmission range. A node may become selfish in particular when its energy and storage resource is constrained. In our ICRP, we choose optimal cutoff threshold r^* and the number of copies is set to 4 for our study. Spray and Wait are stimulated in three cases: One is setting the number of copies to 2 (simulation results using SNW2). The source node will pass the packet to the first encountered node, and the node that has one copy will pass the packet only when it encounters the destination node, which is also a two-hop delivery mechanism. Another is setting the number of copies to 4 (simulation results using SNW4), and this way, we can directly analyze the impact of the value of r. The third case is setting the number of copies to 8 (simulation results using SNW8).

Fig. 9 shows that the delivery probability slowly decreases as the selfishness ratio increases under different numbers of copies; in particular, it obviously decreases when the number of copies is 1, the single-copy scenario.

Figs. 10 and 11 show that, with the increase in selfishness ratio, the performance of Spray and Wait, Epidemic, or PROPHET is significantly affected. The *delivery_prob* significantly decreases, and the *delay_average* gradually increases.

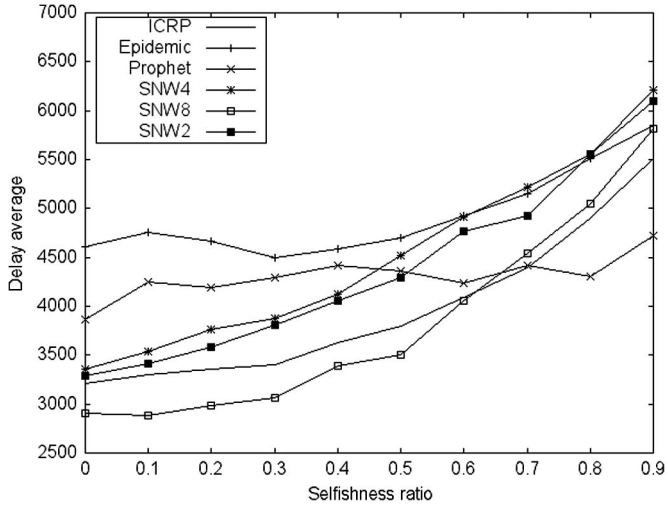

Fig. 11. Comparison of $delivery_{average}$ among ICRP, Spray and Wait, Epidemic, and PROPHET protocols.

ICRP stimulates and selects nodes with certain optimality consideration to forward data rather than blindly choosing relay nodes, and thus, the *delivery_prob* is stable. In Fig. 10, we observe that the curves corresponding to both the Epidemic protocol and the Prophet protocol are increasing when the selfishness ratio is higher than 70% because these two protocols are based on flooding to deliver messages. Flooding should deliver a packet from one node to all other network nodes using as few messages as possible. It is reasonable that the delivery probabilities of the two protocols are low since there are a large number of messages generated and stored in the networks, resulting in less available space to accept new messages when the selfishness ratio is low. In Fig. 11, with the increasing number of the selfishness ratio, SNW2 approaches to the direct delivery, where the source node directly passes message to the destination node, and the *delay_average* does not significantly change when selfishness ratio is smaller than 67%.

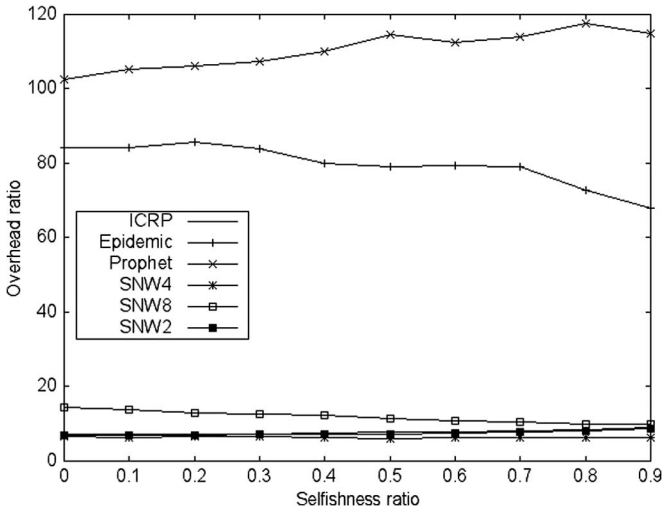

Fig. 12. Comparison of $overhead_{ratio}$ among ICRP, Spray and Wait, Epidemic, and PROPHET protocols.

As shown in Fig. 12, the forwarding times of Epidemic and PROPHET are larger than those of other protocols. Equation (6) shows that the more relayed, the higher the *overhead_ratio*. With the increasing number of the selfishness ratio, the relayed and *delivery_prob* decline; thus, the *overhead_ratio* declines. Since the number of messages generated in the network for a message delivery is larger than others, the overhead is heavy than others. The relayed of SNW2 and SNW4 are relatively less than others; hence, the *overhead_ratio* is lower. Our ICRP can ensure higher *delivery_prob* and lower network load, and thus, it is more suitable for the restricted DTN environments because ICRP can save the network resource with high message delivery ratio.

To sum up, our protocol can defend against selfish behavior when comparing with Epidemic, PROPHET, and Spray and Wait. Moreover, our protocol can achieve higher delivery ratio and lower delay because we no longer blindly choose a relay node, rather than choosing the optimal relay node to ensure message forwarding efficiency, thereby saving network resource even if there exist selfish nodes in the networks.

VI. Conclusion

In this paper, we have developed an ICRP for two-hop DTNs. Based on the theory of optimal sequential stopping in classical secretary problem, we propose an algorithm to select relay node in a certain optimal fashion by considering both the encounter probability among nodes and credit earning transmission cost. We design a payment-based incentive mechanism to stimulate nodes to forward messages while preventing selfish behaviors of nodes. In addition, we make use of bilinear pairing in data transmission to ensure the integrity of message and the security in the payment process.

Experimental results show that our proposed ICRP can effectively stimulate nodes to forward messages while preventing selfish nodes from impacting the performance and achieve better successful delivery ratio while reducing the consumption of network resources compared with the Epidemic, PROPHET, and Spray and Wait protocols.

References

[1] S. Burleigh *et al.*, "Delay-tolerant networking: An approach to interplanetary Internet," *IEEE Commun. Mag.*, vol. 41, no. 6, pp. 128–136, Jun. 2003.
[2] A. Chaintreau *et al.*, "Impact of human mobility on opportunistic forwarding algorithms," *IEEE Trans. Mobile Comput.*, vol. 6, no. 6, pp. 606–620, Jun. 2007.
[3] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The multiple-copy case," *IEEE Trans. Netw.*, vol. 16, no. 1, pp. 77–90, Feb. 2008.
[4] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, pp. 145–158, Oct. 2004.
[5] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: Overview and challenges," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 1, pp. 24–37, 1st Quart. 2006.
[6] K. Fall and S. Farrell, "DTN: An architectural retrospective," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 5, pp. 828–836, Jun. 2008.
[7] H. Yue, H. L. Fu, L. Guo, Y. Fang, and P. Lin, "An efficient prediction-based routing protocol in delay tolerant networks," in *Proc. IEEE GLOBECOM*, Dec. 2013, pp. 4471–4476.
[8] J. Crowcroft, E. Yoneki, H. Pan, and T. Henderson, "Promoting tolerance for delay tolerant network research," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 5, pp. 63–68, Oct. 2008.
[9] A. Lindgren and P. Hui, "The quest for a killer app for opportunistic and delay tolerant networks," in *Proc. ACM CHANTS*, Beijing, China, 2009, pp. 59–66.
[10] P. U. Tournoux, E. Lochin, J. Leguay, and J. Lacan, "Robust streaming in delay tolerant networks," in *Proc. IEEE ICC*, May 2010, pp. 1–5.
[11] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad-hoc wireless networks," in *Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. INFOCOM*, 2001, vol. 3, pp. 1360–1369.
[12] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks," in *Proc. IEEE WCNC*, Mar. 2004, pp. 825–830.
[13] P. V. Moerbeke, "An optimal stopping problem with linear reward," *Acta Mathematica*, vol. 132, no. 1, pp. 111–151, Jul. 1974.
[14] N. Nissan, T. Roughgarden, E. Tardos, and V. Vaziriani, "Algorithmic game theory," *Kybernetes*, vol. 53, no. 7, pp. 78–86, 1972.
[15] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, Mar. 1961.
[16] E. H. Clarke, "Multipart pricing of public goods," *Pub. Choice*, vol. 11, no. 1, pp. 17–33, Fall 1971.
[17] T. Groves, "Incentives in teams," *Econometrica*, vol. 41, no. 4, pp. 617–663, Jul. 1973.
[18] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The single-copy case," *IEEE Trans. Netw.*, vol. 16, no. 1, pp. 63–76, Feb. 2008.
[19] U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in DTNs," in *Proc. IEEE 16th Conf. Netw. Protocols*, 2008, pp. 238–247.
[20] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.
[21] M. Onen, A. Shikfa, and R. Molva, "Optimistic fair exchange for secure forwarding," in *Proc. IEEE 4th Annu. Int. Conf. MobiQuitous*, Aug. 2007, pp. 1–5.
[22] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1483–1493, Apr. 2010.
[23] B. B. Chen and C. Mun Choon, "MobiCent: A credit-based incentive system for disruption tolerant network," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[24] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Int. Conf. Mobile Comput. Netw.*, vol. 4, no. 7, pp. 255–265, 2000.
[25] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the confidant protocol cooperation of nodes: Fairness in dynamic ad-hoc networks," in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2002, pp. 226–236.
[26] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proc. IEEE Workshop MobiHoc*, 2000, pp. 87–96.
[27] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. IEEE 22nd Annu. Joint Conf. IEEE Comput. Commun. Soc. INFOCOM*, Apr. 2003, pp. 1987–1997.
[28] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *Wireless Netw.*, vol. 13, no. 5, pp. 569–582, Oct. 2007.

[29] T. Tsuruike, K. Tsukamoto, M. Tsuru, and Y. Oie, "A message forward scheduling based on a secretary problem for mobile relay nodes," in *Proc. IEEE 4th Int. Conf. INCoS*, Sep. 2012, pp. 436–442.
[30] A. Khosravi, "An optimal stopping algorithm for delay tolerant routing," Project Rep., Univ. Victoria, Victoria, BC, Canada, 2009. [Online]. Available: http://grp.pan.uvic.ca/~arian/csc551.pdf
[31] D. Wen, Y. Cai, and Z. Li, "Two-hop incentive compatible routing protocol in disruption-tolerant networks," *J. Comput. Appl.*, vol. 33, no. 6, pp. 1500–1504, 2013.
[32] D. Wen, Y. Cai, Z. Li, and Y. Fan, "An incentive compatible two-hop multi-copy routing protocol in DTNs," in *Proc. IEEE 9th Int. Conf. MSN*, Dec. 2013, pp. 140–146.
[33] The ONE. [Online]. Available: http://www.net-lab.kk.fi/tutkimus/dtn/theone/
[34] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advance CRYPTO*, Lecture Notes Computer Science. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.
[35] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and Wait: An efficient routing scheme for intermittently connected mobile networks," in *Proc. SIGCOMM*, 2005, pp. 252–259.
[36] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Dept. Comput. Sci, Duke Univ., Durham, NC, USA, Tech. Rep. CS-200006, 2000.
[37] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *SIGMOBILE Comput. Commun. Rev.*, vol. 7, no. 3, pp. 19–20, Jul. 2003.

Ying Cai (M'14) received the B.S. degree in applied mathematics from Xidian University, Xi'an, China, in 1989; the M.S. degree in applied mathematics from the University of Science and Technology Beijing, Beijing, China, in 1992; and the Ph.D. degree in information security from Beijing Jiaotong University in 2010.

From 2012 to 2013, she was a Visiting Research Scholar with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. She is currently a Full Professor with Beijing Information Science and Technology University. She is also a guest researcher with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing. Her current research interests include cybersecurity, wireless networks, and cryptography algorithms.

Yanfang Fan received the B.S. degree in computer science and technology and the M.S. degree in computer application technology from Northeast Forestry University, Harbin, China, in 2002 and 2005, respectively, and the Ph.D. degree in information security from Beijing Jiaotong University, Beijing, China, in 2011.

She is currently a Lecturer with Beijing Information Science and Technology University. Her current research interests include cybersecurity and access control.

Ding Wen received the B.S. degree in information and computing science from the Agricultural University of Hebei, Baoding, China, in 2011 and the M.S. degree in computer application from Beijing Information Science and Technology University, Beijing, China, in 2014.

He is currently with Beijing Information Science and Technology University. His current research interests include wireless networking and delay-tolerant networks.